FortiAnalyzer 6.2
Incident Response & SOC Automation

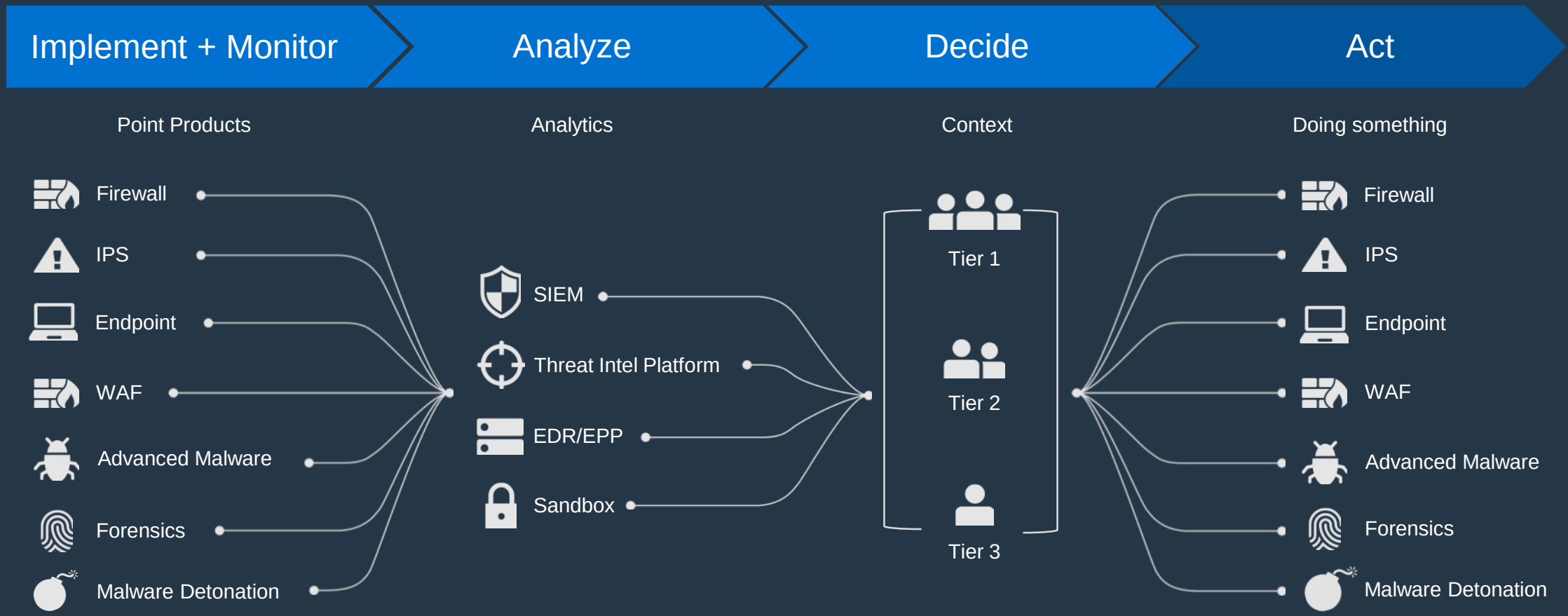
Roland Stierli

In this session you will learn

1. 6.2 Highlights
2. FortiAnalyzer-Cloud & Licensing
3. FAZ Positioning, Sizing & Deployment Use Cases

© Fortinet Inc. All Rights Reserved.

Enterprise Operations



© Fortinet Inc. All Rights Reserved.

Incident Response & Automation

INCIDENT RESPONSE

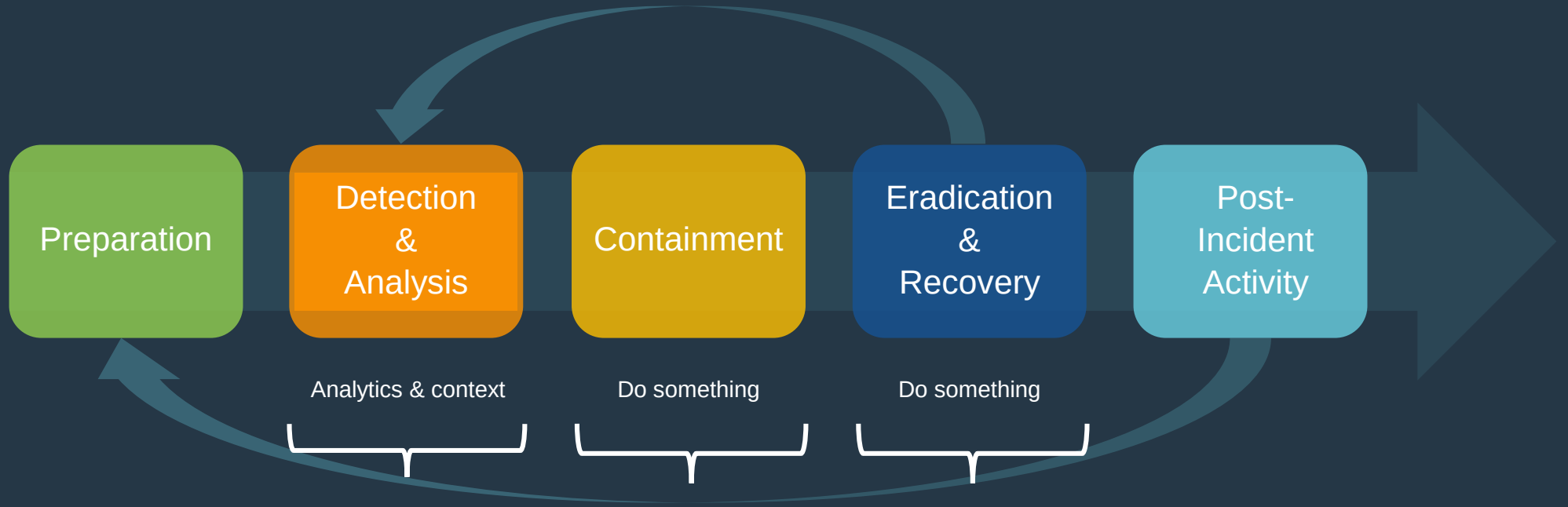
Enabling quick detection, automated correlation and connected remediation

SOC AUTOMATION

Automating manual, time-consuming processes (end-to-end) to offload SOC

© Fortinet Inc. All Rights Reserved.

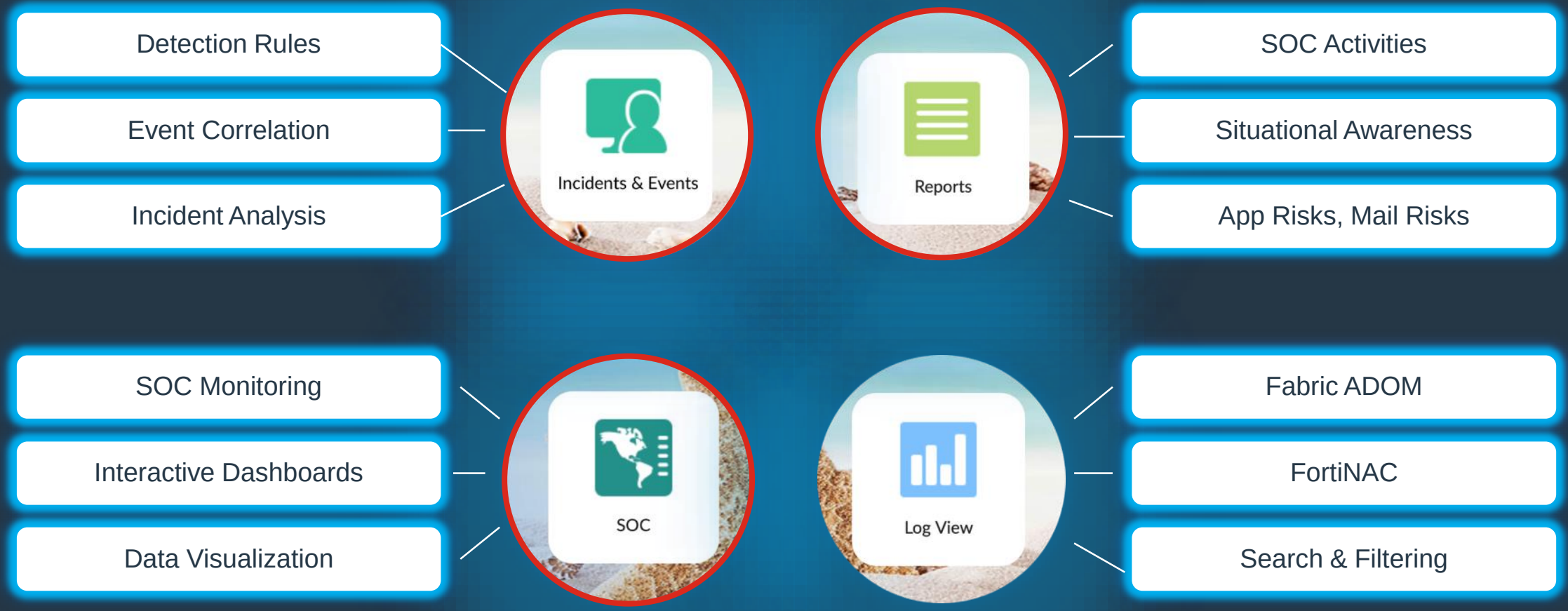
Incident Response Process



Incident Response Process (NIST 800-61r2)

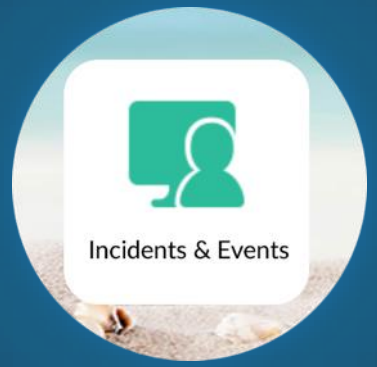
© Fortinet Inc. All Rights Reserved.

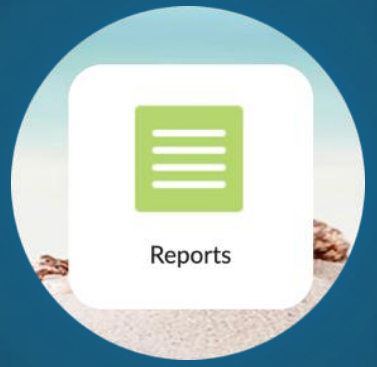
What's New In 6.2?

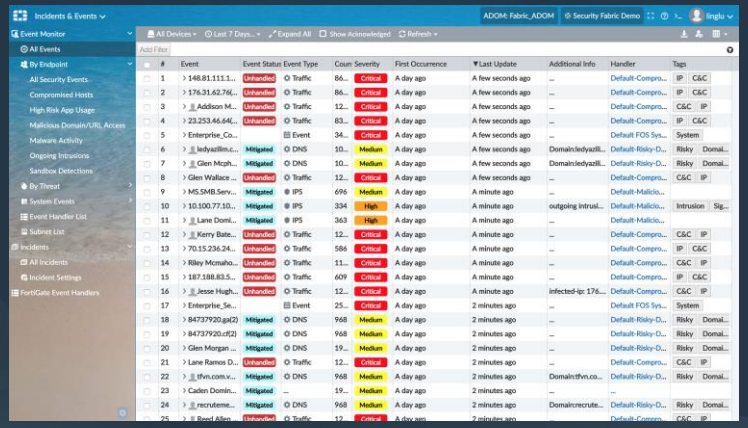


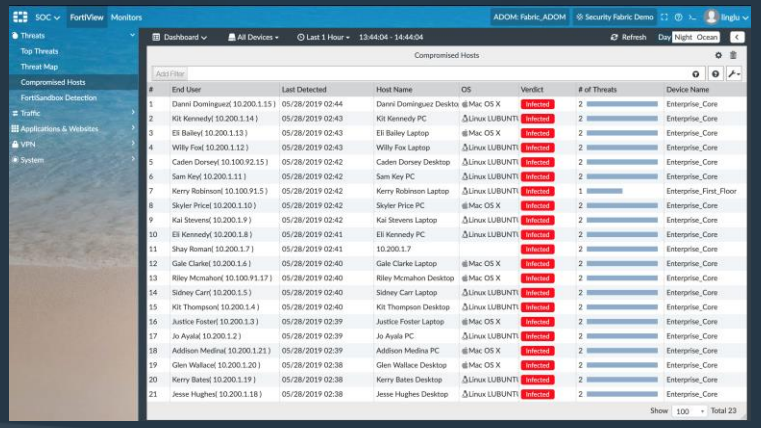
Find out more: Go to FNDN FortiDemo: https://fndn.fortinet.net/index.php?/fortidemo/instances/

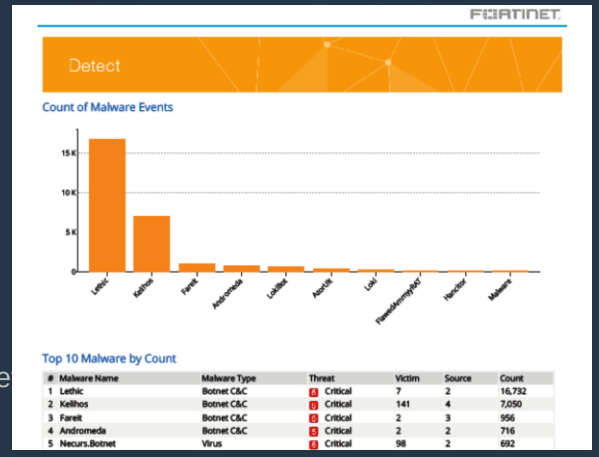
Incident Detection & Analysis





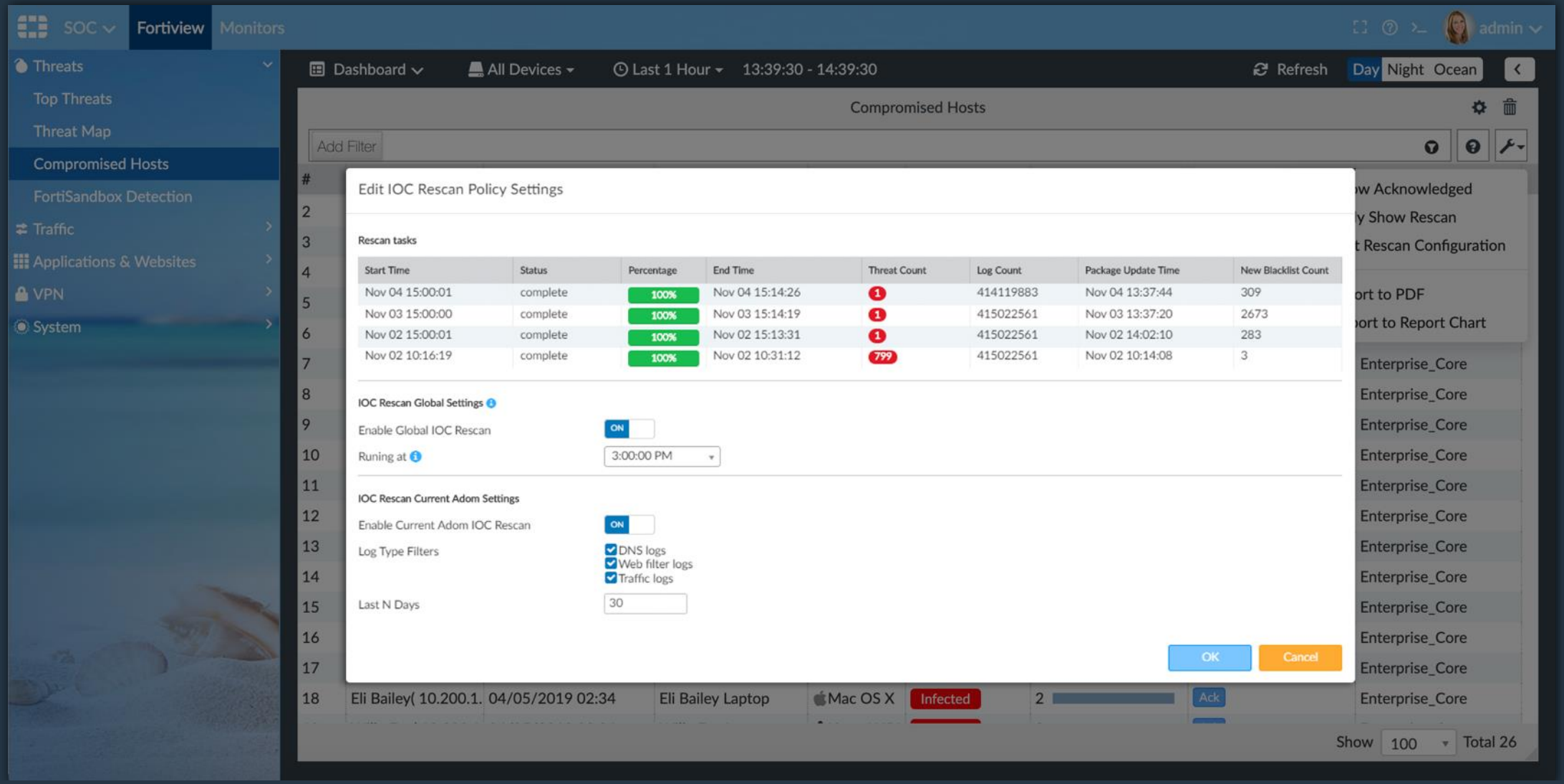






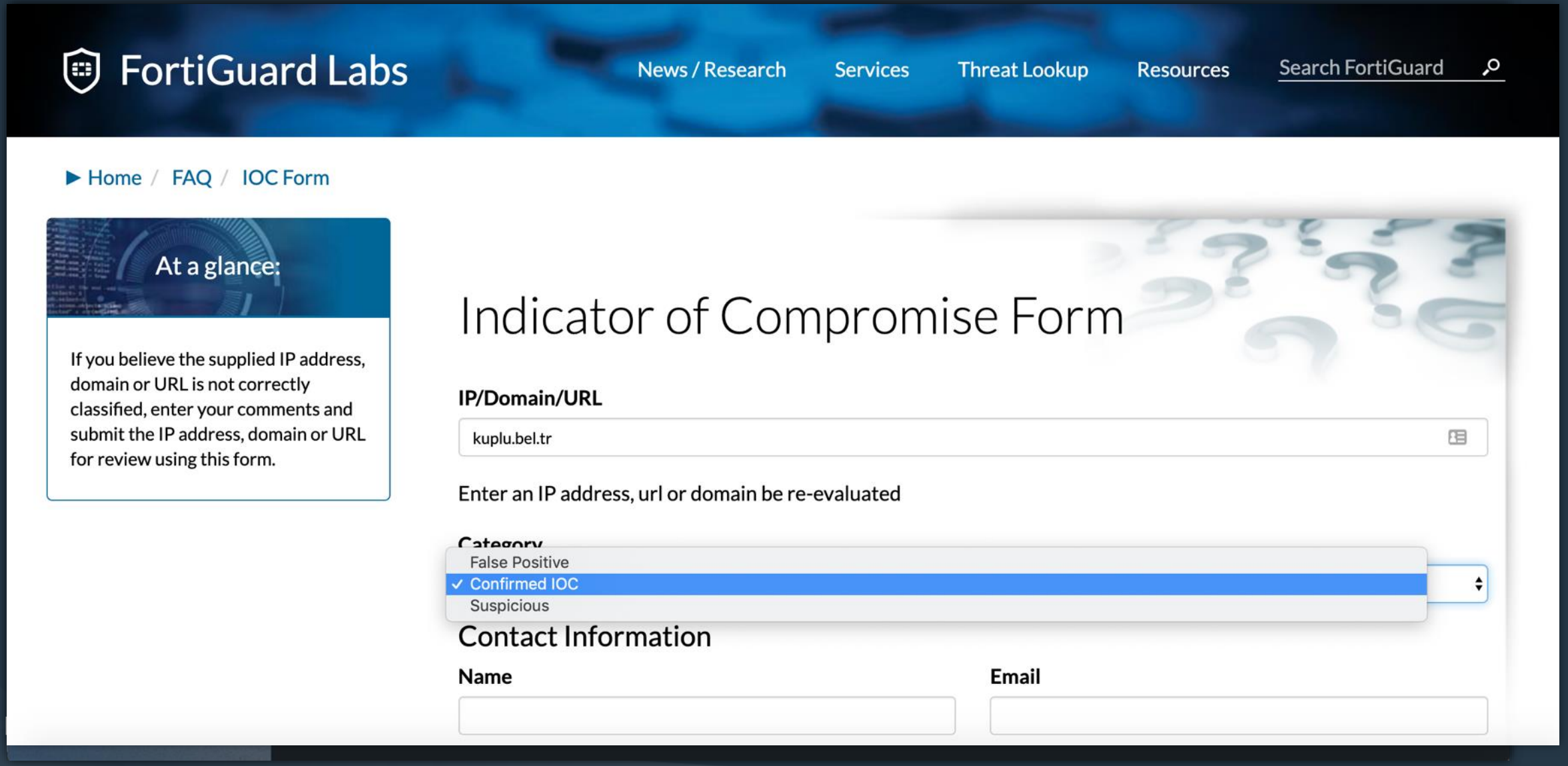
© Fortine

Incident Detection & Analysis – IOC History Scan

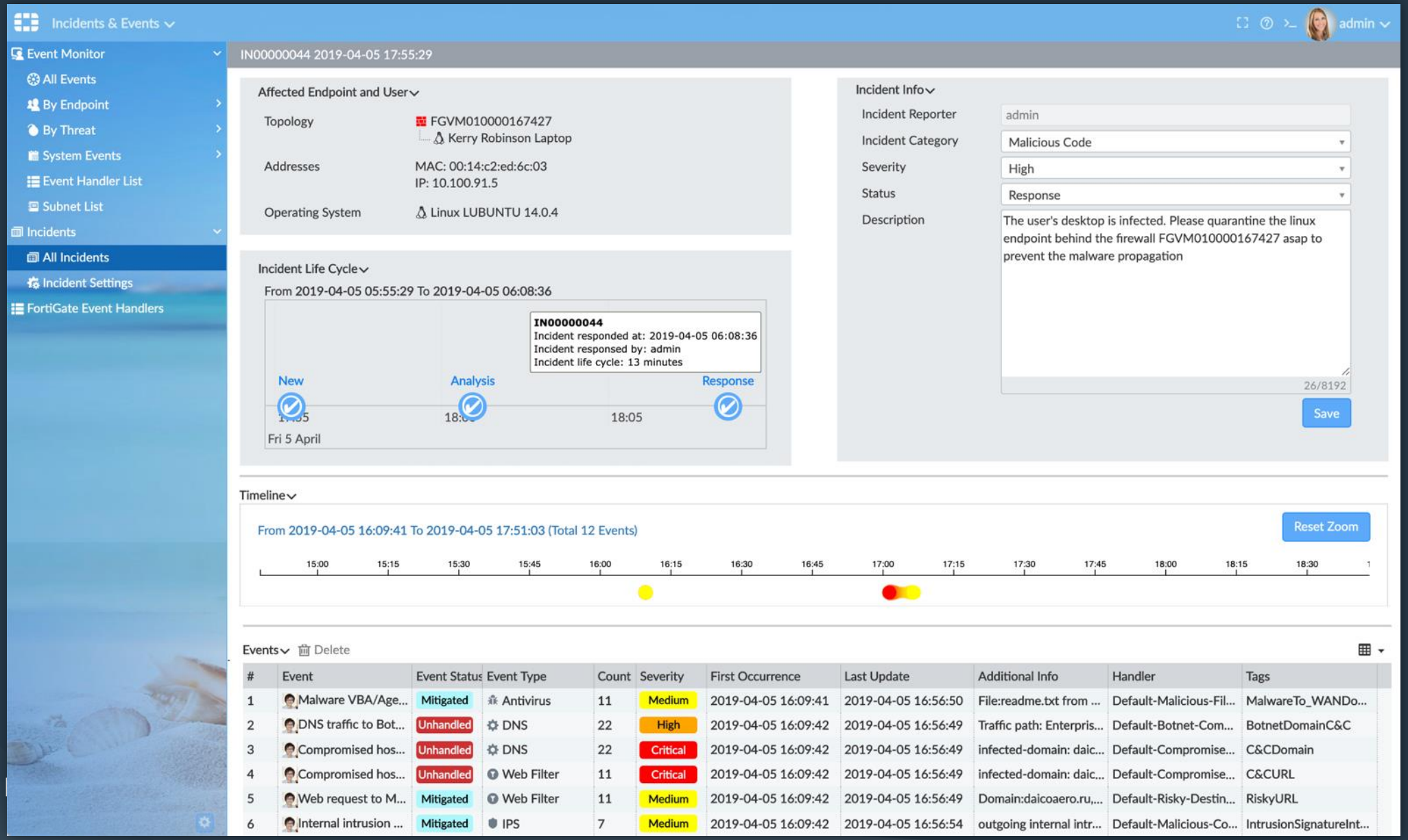


Find out more about IOC: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/779346/how-ioc-works

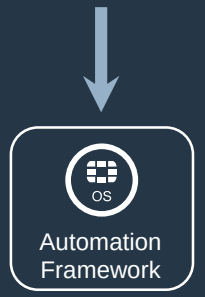
Incident Analysis – Threat Intel Lookup

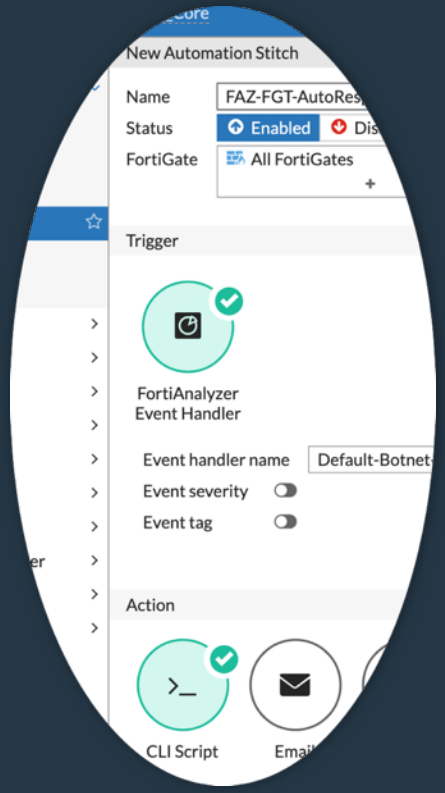


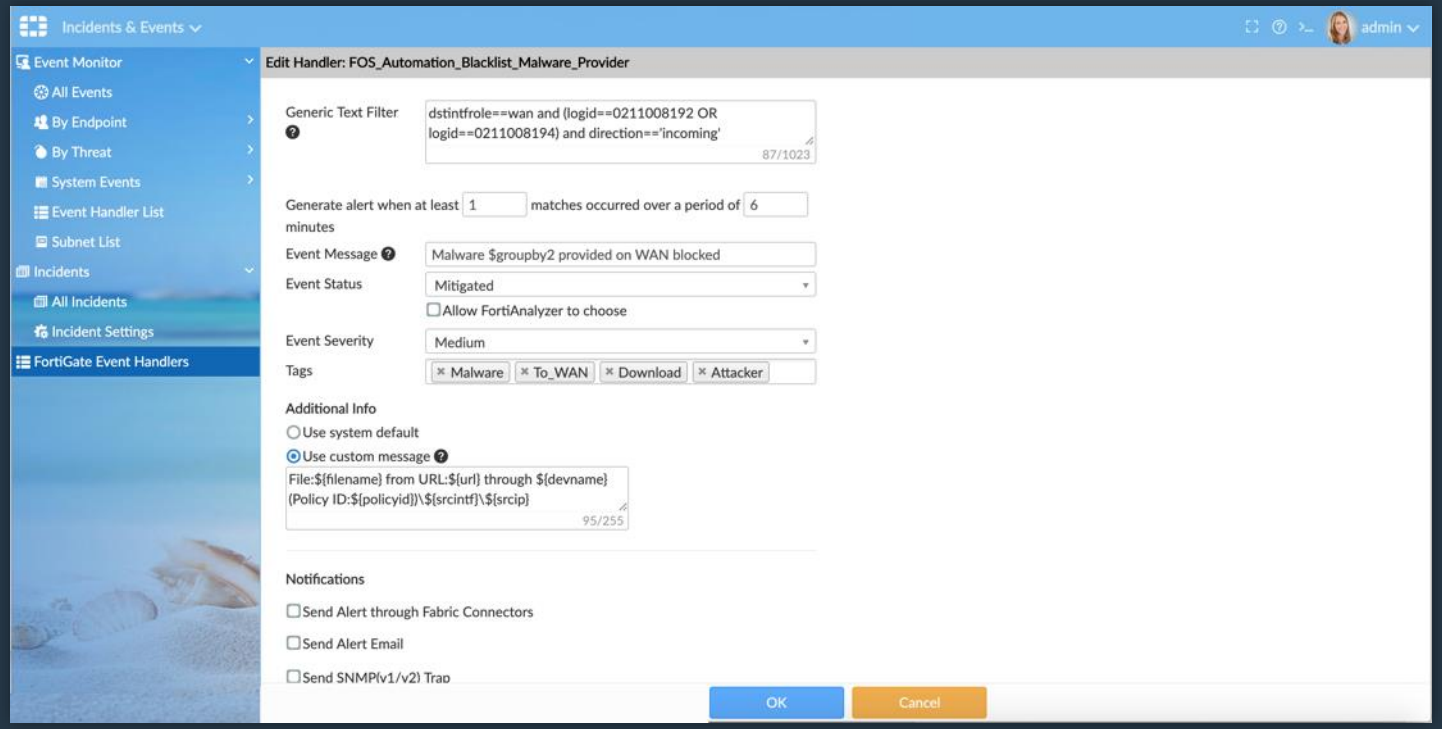
Incident Analysis – Timeline and Life Cycle



Automate Incident Containment (FAZ <-> FOS)

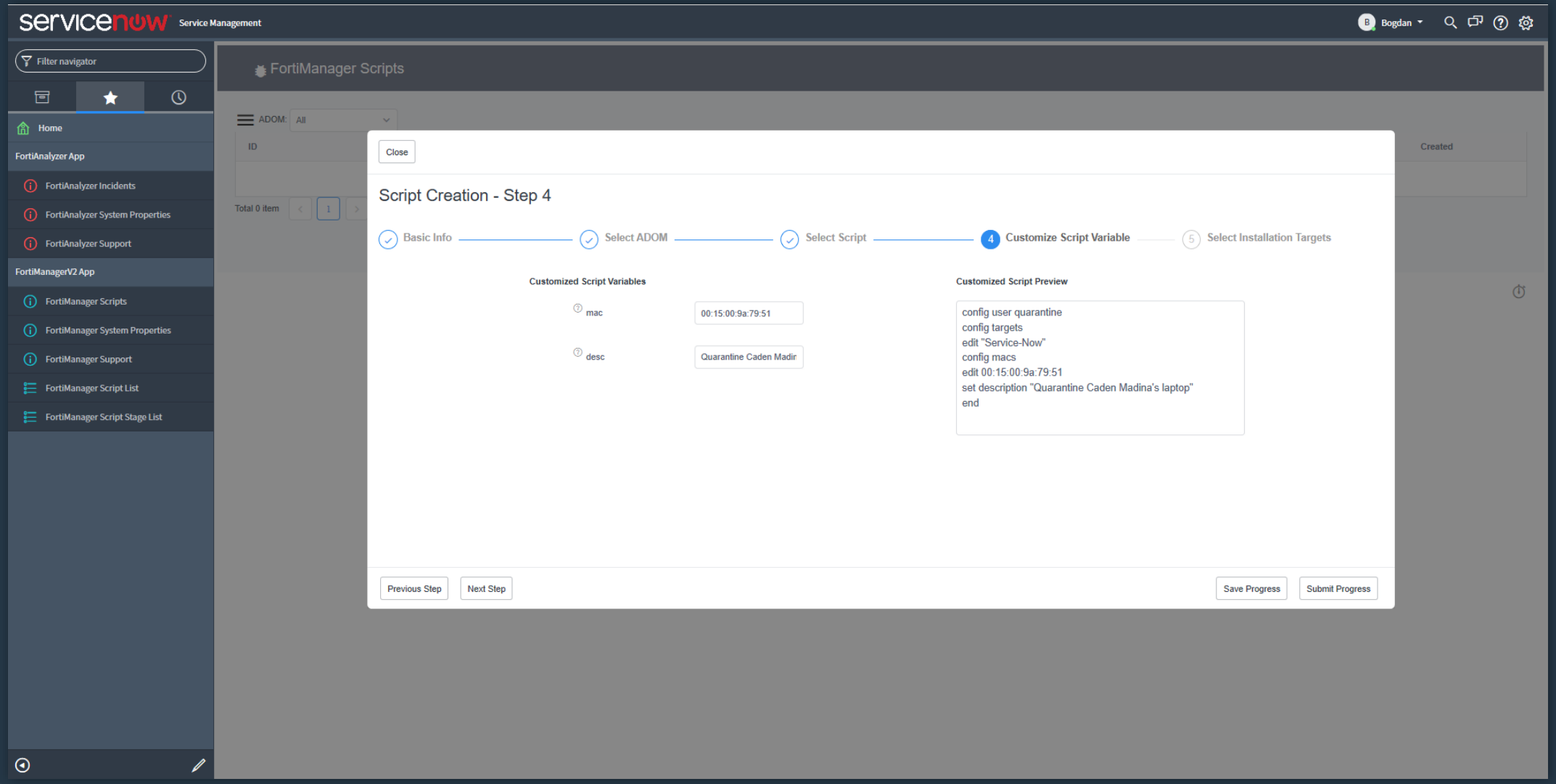






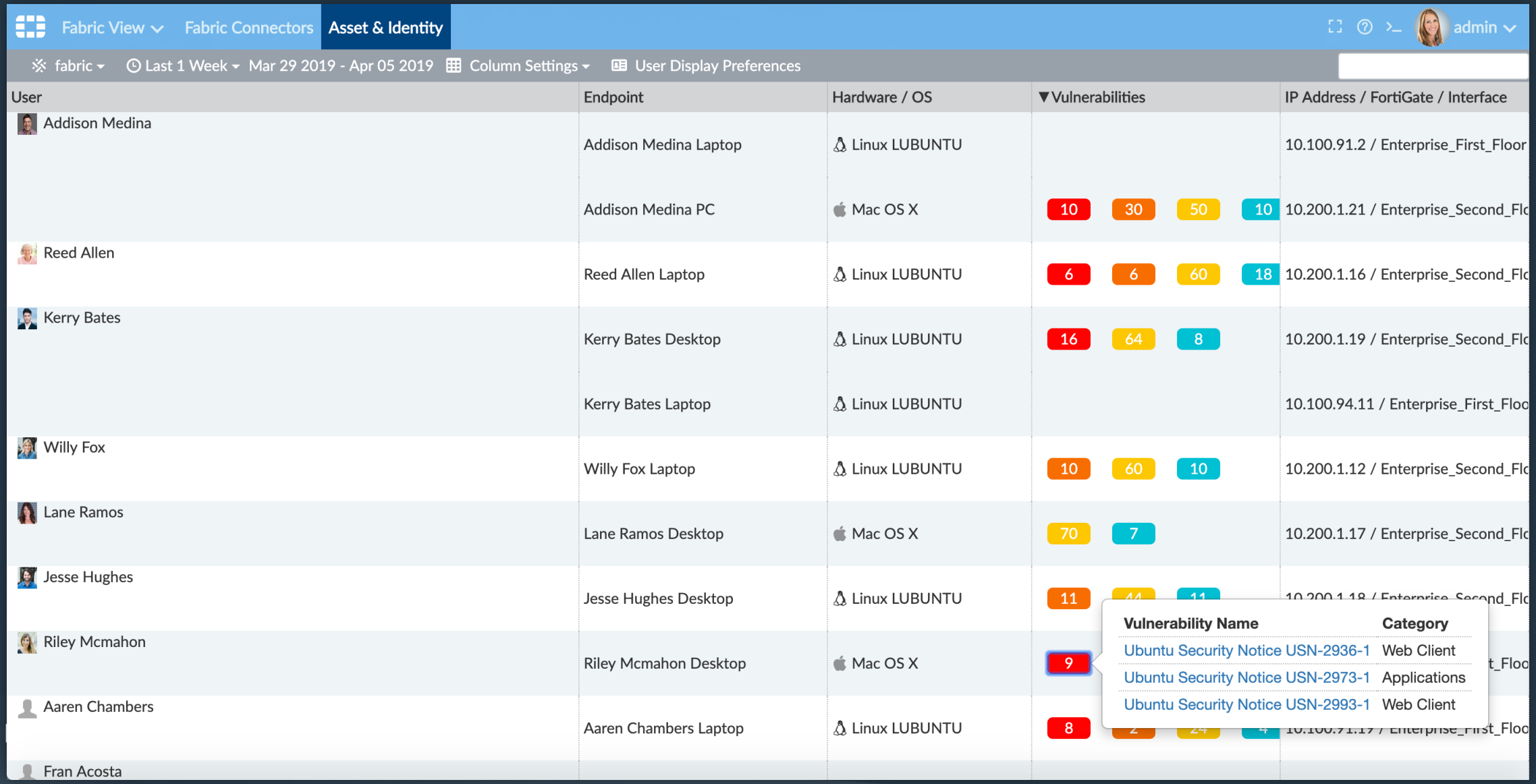
© Fortinet Inc. All Rights Reserved.

Automate Incident Management End-to-End with ITSM

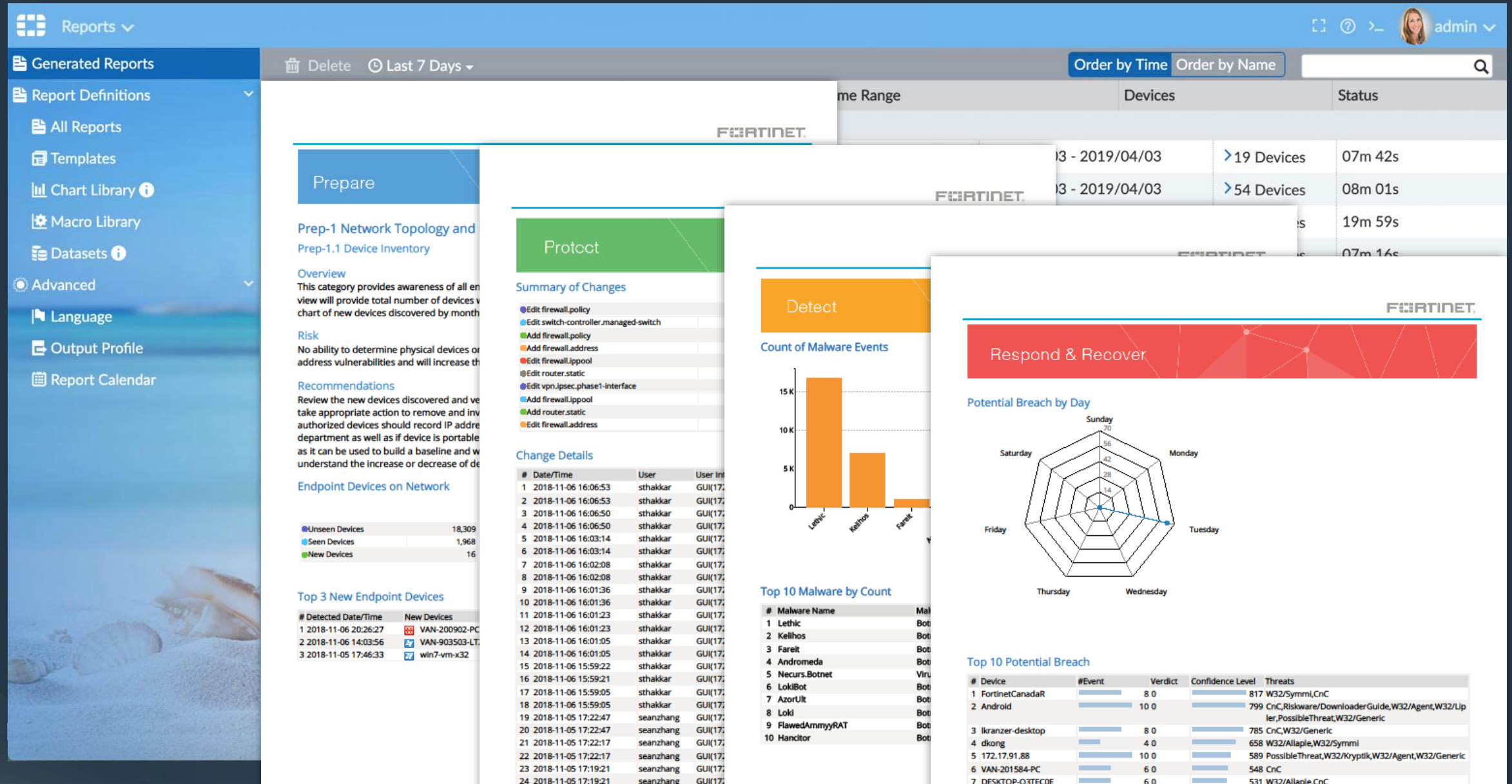


© Fortinet Inc. All Rights Reserved.

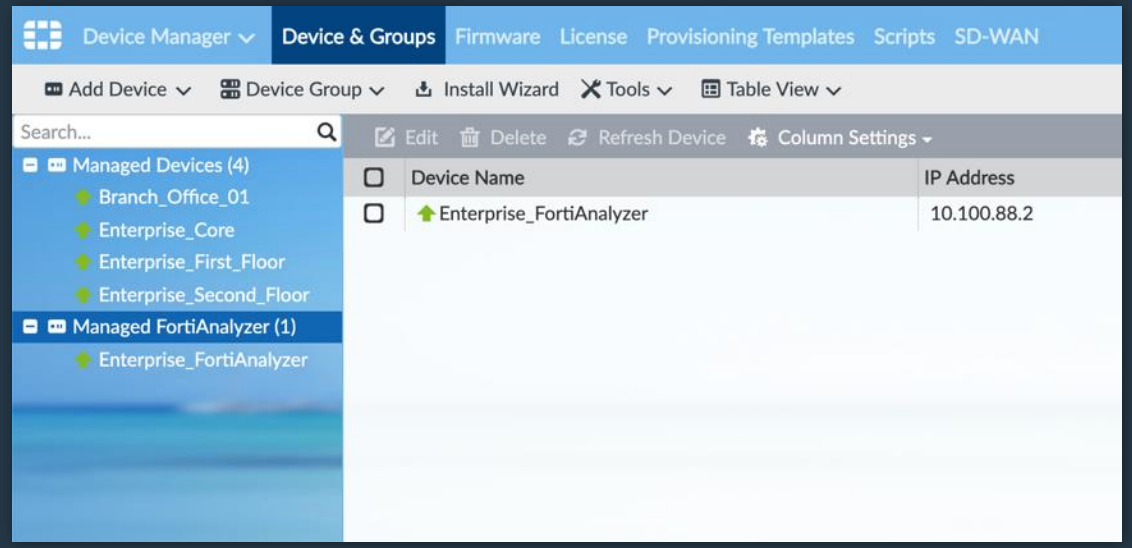
Incident Eradication & Recovery

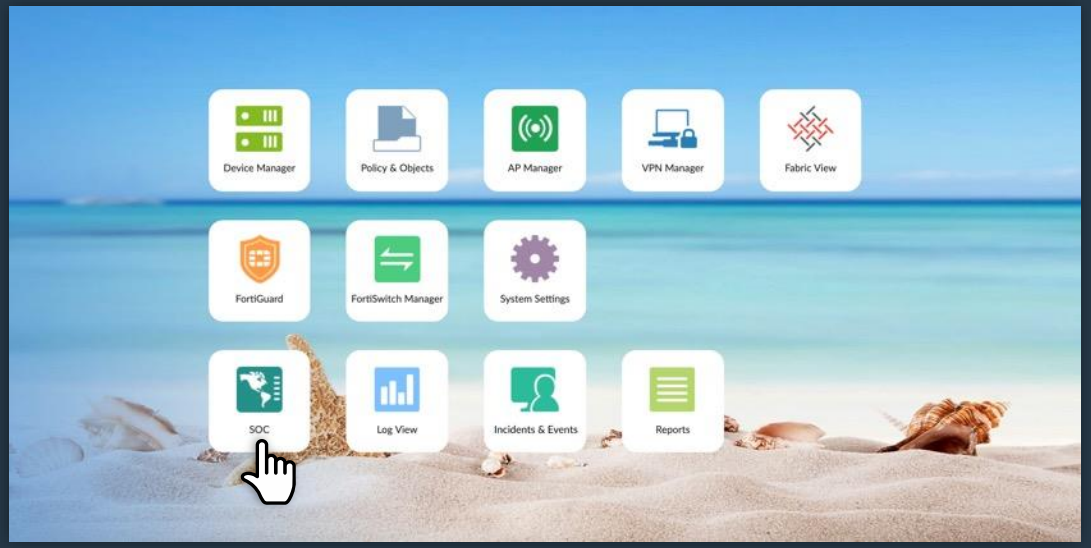


Automate Incident Eradication & Recovery



Single-Pane Visibility – SOC & NOC





© Fortinet Inc. All Rights Reserved.

Q & A

© Fortinet Inc. All Rights Reserved.


FORTINET